

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

**IN THE MATTER OF THE SEARCH OF:
Johnny R. Baker and the premises located
at 941 Ed Davis Road, Wellston, OH 45621,
including any outhouses, vehicles, and
digital devices located on the premises**

Case No. 2:23-mj-635

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

The undersigned, Benjamin Schild, being first duly sworn, deposes and states as follows:

1. I am an Inspector with the United States Postal Inspection Service (hereafter "USPIS") and have been since December 2019. I am currently assigned to the Mail Fraud team in the Cincinnati Field Office. In this capacity, I investigate criminal matters that are connected to the mail, including money laundering and various types of fraud. Prior to my employment with the USPIS, I served as a Special Agent in the United States Secret Service for 12 years. I have received training and investigative experience in interviewing, arrest procedures, search and seizure, search warrant applications, electronic media, and computer investigations, especially as they relate to white collar crime.

2. This affidavit is being submitted in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure authorizing the search of Johnny R. Baker (hereinafter "BAKER"), and the premises known as 941 Ed Davis Road, Wellston, OH 45621, hereinafter the "PREMISES," further described in Attachments A and B, for the things described in Attachment C.

3. I am familiar with the facts and circumstances of this case. The information contained in this affidavit is either personally known to me, based upon surveillance, my interviews of various witnesses and review of various records and publicly available information, or information that has been relayed to me by other agents or sworn law enforcement personnel. Because this affidavit is provided for the limited purpose of establishing probable cause to support a search warrant, I have not included all details I know about this investigation, but rather, I have set forth only those facts that I believe are necessary to establish probable cause.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud) have been committed by BAKER. There is also probable cause to believe that there exists evidence, fruits, and instrumentalities of such violations on the person of BAKER and at the PREMISES.

PROBABLE CAUSE

5. In July 2023, the USPIS initiated an investigation of BAKER, a fireman for the Coalton Volunteer Fire Department in Coalton, Ohio (the “Fire Department”), and an Assembly Specialist for PACCAR, Inc., for suspected violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1956 (Laundering of monetary instruments) and 18 U.S.C. § 641 (Public Money, Property or Records). Based on various records received during this investigation, BAKER appears to have served many roles during his tenure with the Fire Department, most notably as Secretary/Treasurer, Assistant Fire Chief, and, as of January 2023, Fire Chief.

A. The evidence suggests BAKER has significant personal debts and pays many personal expenses with a credit card in the name of the Fire Department.

6. Records indicate BAKER has multiple personal bank accounts with WesBanco, including accounts ending in x6362, and a Home Equity Line of Credit (HELOC).

7. According to bank statements from the WesBanco account ending in x6362, BAKER receives approximately \$3,000 a month from his employer PACCAR, which he uses primarily to pay down several debts (e.g., student loans, tractor payments, HELOC payments, credit card payments, auto loans, etc.).

8. Records from First National Bank of Omaha (FNBO) show that BAKER also controls a business credit card ending in x0421, which was opened in 2010 and is held in the name of the Fire Department and BAKER himself (the “Fire Department Credit Card”). BAKER did not qualify for the card on his own and had to have someone co-sign on his behalf. The Fire Department Credit Card statements and application depict BAKER (using his personal address) as the authorized signer/company representative on the account. As explained more fully below, BAKER appears to use the Fire Department Credit Card to pay personal bills and make personal purchases, and the credit card bills are funded by money donated to the Fire Department.

B. The evidence suggests BAKER engaged in an embezzlement scheme to conceal and personally benefit from donations being made to the non-profit Fire Department.

9. Jackson County, Ohio is a relatively rural community that depends on several fire departments throughout the county for various emergency/medical needs. During this investigation, through research and surveillance, I learned that BAKER has worked for the Fire Department since 2009, and over the course of several years he has

implemented a “pull-tab” gaming system in several local convenience stores throughout Jackson County. These games of chance allow residents and commuters an opportunity to win money. The implementation of the pull-tab machines is financially beneficial for both the businesses and the Fire Department and is conducted in the following way:

- a. BAKER provides local convenience stores with a pull-tab gaming system, typically purchased by the Fire Department through Lancaster Bingo Company.
- b. Convenience stores sell tabs to local customers and all proceeds go directly to the Fire Department.
- c. Funds are deposited by BAKER into a Fire Department WesBanco business checking account, ending in x2798 (the “WesBanco x2798 Account”).
- d. BAKER re-imburses or pays convenience stores their monthly winnings from the WesBanco x2798 Account.
- e. BAKER transfers remaining pull-tab proceeds to a WesBanco business checking account, ending in x9043, also in the name of the Fire Department (the “Wesbanco x9043 Account”).

The below chart gives an example of how much money has been deposited, withdrawn, and transferred by BAKER:

	2020	2021	2022	2023 (thru July)	Totals
Deposits into WesBanco x2798 Account from convenience stores	\$638,434.04	\$665,497.50	\$515,253.27	\$288,671.59	\$2,107,856.40
Winnings paid back to stores	\$309,043.00	\$285,580.86	\$265,783.30	\$122,286.95	\$982,694.00

Transfers from WesBanco x2798 Account to WesBanco x9043 Account	\$330,000.00	\$395,000.00	\$246,000.00	\$135,000.00	\$1,106,000.00
---	--------------	--------------	--------------	--------------	----------------

10. Once the funds are transferred to the WesBanco x9043 Account, BAKER uses some of the money to pay for the needs of the Fire Department. But he also uses the money to benefit his personal lifestyle. The examples below show how BAKER has utilized the money being transferred to the WesBanco x9043 Account:

- a. Making payments on bills and debts for the Fire Department (e.g., gas, electric, cable, fire truck payments, gear, pest control, insurance, or withdrawing cash for bingo games the fire department puts on at the local event center). Approximately \$470,000 of the funds paid for one engine, one tanker, one rescue, and one custom built brush truck.
- b. Making apparently personal Amazon purchases, including for parts associated to a 2021 Polaris RZR 1000 UTV (i.e., a heavy-duty ATV) belonging to BAKER, and other household items, totaling \$12,156.69. Below are some examples of BAKER using the WesBanco x9043 Account to make such Amazon purchases:

1. KEMIMOTO XP 1000 Lower Door Inserts, UTV Lower Half Doors Panels Compatible with 2014-2023 Polaris RZR XP 1000 S 900 Turbo 60" Models OEM Style Frame Replacement (2 Doors) OEM 2879509

2. KIWI MASTER Hard Roof Top Compatible for 2014-2023
Polaris RZR XP 1000 Accessories 900 S Turbo 2 Door UTV
Top Black with LED Lighting
 3. Galena SD 2BBT4B -Polaris RZR Stereo BT Radio 08-14 RZR
2-Seater only
 4. SuperATV Rear Windshield for Polaris RZR XP 1000 (2014-
2023) | USA Made | Made of 1/4" Polycarbonate- 250x stronger
Than Glass | Easy to Install | Protects Against Flying Mud and
Debris
 5. SuperATV Deluxe Turn Signal Kit for Polaris RZR XP 4 Turbo
(2016-2018) | Dash Mounted Turn Signal Rocker Switch | Plug
and Play Installation.
 6. Hessaire MC18V Portable Evaporative Cooler, Green, 1300
CFM, Cools 500 Square Feet
 7. RAREELECTRICAL New Counterclockwise Starter
Compatible with Honda Gx630 Gx630H Gx630R Engines by
Part Numbers 428000-6410 31200-Z6L-003 4280006410
31200Z6L003
 8. Sifely Smart Lock, Keyless Entry Door Lock, Smart Door Lock
with Handle, Smart Lock for Front Door, Keyless Door Lock,
Fingerprint Door Lock, Biometric Door Lock, Keypad Door
Lock, Digital Door Lock
- c. Spending \$4,066.76 in purchases at Sam's Club in Chillicothe, Ohio.

- d. Making over \$225,000 in payments via check or online for the Fire Department Credit Card.

C. The evidence suggests BAKER embezzled Fire Department funds.

11. According to a review of credit card statements, BAKER made approximately \$196,000 in personal expenditures on the Fire Department Credit Card from 2020 through July 2023, including the following:

- a. \$29,080 in cash withdrawals, while being charged a \$15 cash advance fee for each transaction.
- b. \$5,224.90 for two Carnival cruises for BAKER, his two children and what is believed to be his girlfriend and one of her children.
- c. \$5,818 in purchases using a linked PayPal account.
- d. \$14,694.96 in apparently personal Amazon purchases. Below are a few examples of the various types of items:
 - 1. Apple AirPods Pros
 - 2. REPTI ZOO 67Gallon Reptile Large Terrarium Upgrade Glass Front Opening Tank Sliding Door with Screen Ventilation Reptile Terrarium About 48" x 18" x 18"(Knock-Down)
 - 3. SAXX Men's Underwear – VIBE Boxer Briefs with Built-In BallPark Pouch Support – Pack of 2, Black/Hot Cocoa Hot Tub,XX-Large
 - 4. GoPong 8 Foot Portable Beer Pong/Tailgate Tables (Black, Football, American Flag, or Custom Dry Erase)
 - 5. SuperATV Black Ops 4500 lb Winch with Winch Mounting Plate for 2019-23 Polaris RZR XP 1000 / XP 4 1000 | Complete

Winch Kit Ready for Install | Powder Coated Heavy Duty Steel
Plating

6. SUPER DEAL PRO 61-inch 2in1 Large Bird Cage with Rolling
Stand Playtop Parrot Chinchilla Finch Cage Macaw Conure
Cockatiel Cockatoo Pet House Wrought Iron Birdcage, Black
 7. Electric Gel Ball Blaster, Vkifun Automatic Splatter Ball
Blaster Toy Gun with 30000 Water Beads and Goggles,
Outdoor Activities Shooting Team Game for Ages 8+ Boys &
Girls Gifts
 8. Trupedic x Mozaic - 8-inch Full Size Standard Futon Mattress
(Frame Not Included) | Basic Silver | Great for Kid's Rooms or
Guest Areas - Many Color Options
- e. \$626.40 for Pirate Parasailing in Virginia Beach, VA for BAKER, his
children, and three of their friends.
 - f. \$4,384.97 for a 6-day / 5-night stay at Wilderness at the Smokies and
Soaky Mountain Waterpark for BAKER, his children, and what is
believed to be his girlfriend and her children.
 - g. \$3,185.00 for a rental of a charter bus.
 - h. \$560.18 from Chillicothe Fireworks.
 - i. \$1,317 for three Southwest Airlines plane tickets.
 - j. \$1,125 for Cincinnati Reds tickets associated to the charter bus rental
(for BAKER's son's birthday).
 - k. \$7,294.63 on payments toward the 2021 Polaris RZR 1000 UTV.

- l. \$576.95 for King's Island tickets and Fast Passes.
- m. \$1,313.77 for a firearm and ammunition.
- n. \$1,083.81 for a Get-Away Cabins vacation rental.
- o. \$3,174.59 for electric bill payments to his personal residence.
- p. \$1,419.82 for auto insurance payments on his vehicle and Polaris UTV policies.
- q. \$6,243.11 in purchases made at the Sam's Club in Chillicothe, Ohio.
- r. \$2,984.50 in purchases made at the Wal-Mart in Jackson, Ohio.
- s. \$1,431.09 in purchases made at the Sam's Club in Coalton, Ohio.
- t. \$929.78 in purchases on OnlyFans (a paid social media content site).
- u. \$8,297.19 in purchases for stays at the Kalahari Resort in Sandusky, OH.
- v. Thousands of dollars in purchases on clothing and apparel.
- w. Thousands of dollars in purchases at Menard's, Harbor Freight, Rural King, Lowes, and other hardware stores.
- x. Thousands of dollars in purchases for hotels, restaurants, gas, sporting events, concerts, airline travel, pets and their insurance/accessories, Spectrum cable, water bill, iPhone payments, and other items associated to BAKER.

SEARCH LOCATIONS

12. Based on research and documents provided over the course of the investigation, extensive evidence of the fraud scheme is likely to be found on the person of BAKER and at the PREMISES (i.e., BAKER's residence). The PREMISES is the primary mailing address for the Fire Department Credit Card, which suggests that

statements and other bookkeeping records related to Fire Department funds are likely to be located there. Dozens of items purchased with the Fire Department Credit Card, and ultimately funded by Fire Department funds in the WesBanco x9043 Account, are likely to be located at the PREMISES, including, for example, the Polaris UTV and personal items purchased on Amazon. There are also likely to be photographs of BAKER or his family enjoying vacations or other events paid for by Fire Department funds. Such evidence is also likely to be on BAKER's cell phone, which is likely to be found on BAKER's person.

13. Based on my training and experience in investigations of wire fraud, embezzlement, and money laundering, I know that it is common for individuals involved in such crimes to maintain records of their criminal activities in the form of books, paper notes, notebooks, computer files, telephone texts, digital address books, or papers, and that such documents and or electronics are often stored at their personal residence.

14. I have participated in the execution of multiple search warrants involving the seizure of bank records, books and records, false and fraudulent documents, and computer hardware and software. From my training and experience, I know that it is common for individuals involved in fraudulent activity to maintain records including, but not limited to the following at their personal residences:

- a. Bank records; credit card account records; brokerage account records; investment records; financial institution records; and other records reflecting the receipt of income, transfer of assets, or expenditure of income produced by the businesses.

- b. Business or personal records related to the receipt, transfer, and expenditure of income received from the business.
- c. Records and/or documents memorializing the sale/distribution of their product or the providing of services.
- d. Records and/or documents provided to customers in connection with the services or product.
- e. Correspondence to and/or from actual or prospective customers.
- f. Identification records, including personal identifying information of other individuals.
- g. Documents which have been altered from their original state; and
- h. Other records and/or documents which appear to be related to the business including, but not limited to notes, internal correspondence, external correspondence, and memoranda.

15. Persons engaged in financial crimes often maintain such records for long periods of time, particularly when they are involved in ongoing criminal conduct over a long period of time. There are many reasons why criminal offenders maintain evidence for long periods of time. First, to the offender, the evidence may seem innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered

in light of other evidence. Second, the criminal offender may no longer realize he still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. Third, the criminal offender may also be under the mistaken belief that he has deleted, hidden or further destroyed computer-related evidence, which in fact, may be retrievable by a trained forensic computer expert.

Computers, Electronic Storage, and Forensic Analysis

16. As described above and in Attachment C, this application seeks permission to search for records that might be found at the PREMISES or on BAKER in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media (which includes a smartphone or cellular telephone). Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

Storage of Records Electronically

17. I submit that if a computer or storage medium is found on the PREMISES or on BAKER, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes"

a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

Forensic Evidence: Deleted Files, User Attribution Evidence

13. As further described in Attachment C, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premise or on BAKER because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This

“user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to commit internet fraud, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain the following: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

18. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media.

Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search and what tools or

knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

19. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

20. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

21. Based on the foregoing facts, I believe probable cause exists to believe that BAKER has committed violations of 18 U.S.C. § 1343 (Wire Fraud).

22. Based on my knowledge, training, experience, and the investigation to date, I submit that there is probable cause to believe that the person and property to be searched as further described in Attachments A and B contain evidence, as further described in Attachment C.

23. Based on the facts contained in this affidavit, I request that the Court issue the proposed search warrant under Federal Rule of Criminal Procedure 41 to search the locations described in Attachments A and B and to seize those items set forth in Attachment C, which constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. 1343 (Wire Fraud).

Respectfully submitted,

Benjamin Schild


Benjamin Schild,

Inspector

United States Postal Inspection Service

Subscribed and sworn to before me on this 9th day of November, 2023.

Elizabeth A. Preston Deavers
Elizabeth A. Preston Deavers
United States Magistrate Judge

The seal of the United States District Court for the Southern District of Ohio is visible in the background. It features an eagle with spread wings, perched on a shield with vertical stripes. The text "UNITED STATES DISTRICT COURT" is arched above the eagle, and "SOUTHERN DISTRICT OF OHIO" is arched below it.

ATTACHMENT A

Premises to Be Searched

1) The PREMISES is a double wide mobile home located at 941 Ed Davis Rd, Wellston, OH 45621 in Jackson County, OH. The house has a light brown roof and yellow colored siding, to include green window shutters. The front door is white, and the house can be identified by the numeric address, 941, on the light brown plastic mailbox located in front of the residence. The residence also contains a gray shed/outhouse with a blue roof and white front door.





ATTACHMENT B

Person to Be Searched

Johnny R. BAKER is a white male with brown hair and blue eyes, standing approximately 6'1" tall and weighing approximately 255 pounds. He is 37 years old and resides at 941 Ed Davis Rd, Wellston, OH 45621. His picture is below.



ATTACHMENT C

Particular Things to Be Seized

For the period of January 1, 2018, to the present, the following items (whether in paper or electronic form) related to the following individuals or the following businesses (or any variations of thereof):

- Johnny Baker
- Coalton Volunteer Firemen, Inc. (the “Fire Department”)

as may constitute fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud).

1. All personal and business (including the Fire Department) financial records including:
 - A. Currency in excess of \$1,000 and other monetary instruments; bank records, including bank statements, passbooks, deposit slips, deposit items withdrawal slips, cancelled checks, credit and debit cards, credit card records, bank receipts, bank checks, money orders and receipts, wire transfer records, credit and debit memos, safe deposit box records and keys, money wrappers, fictitious identification, and other items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money;
 - B. Liability records including loan documents and correspondence with lenders; letters of credit, promissory notes, contracts, mortgages, note agreements, loan or credit applications, payment schedules/records, security interests, and loan interest computations;
 - C. Bookkeeping/accounting records and supporting source documents relating to receipts and expenditures including daily sheets, general ledgers, general journals, accounts and notes receivable, accounts and notes payable, balance sheets, income statements, statements of profit and loss, check registers, invoicing records, receipt books and “in-house” financing records;
 - D. Investment records including statements and reports; receipts for the purchase, transfer or sale of stocks, bonds and other securities; documents related to brokerage accounts and shares of stock; correspondence and memoranda to/from any investment firm or financial advisor; and
 - E. Expenditure records including check registers, bills, receipts and invoices, balance sheets, ledgers and notes;

2. All personal and business (including the Fire Department) tax records for the years January 1, 2017 – Present including all federal, state, and local tax returns, together with all schedules and attachments; drafts, copies and partially completed returns; tax preparation files including receipts, work papers, and notes; and correspondence to/from or regarding any tax authority, return preparer, or accountant;
3. Documentation of business ownership, organization and control including Secretary of State filings, articles of incorporation, partnership agreements, applications for an EIN, and meeting minutes;
4. Employment records including employment applications, contracts, Forms W-2 or 1099, timesheets, time cards, paychecks and/or paystubs, hiring and/or termination notices, position descriptions, employee personnel files;
5. All records of purchase, sale, ownership and control of assets such as boats, vehicles, real property, jewelry, electronics, precious gems and metals, furs, household/business furnishings, and other assets or items of significant value reasonably believed to be proceeds of the illegal activity described in the affidavit for this search warrant. Such records include purchase/sale contracts, invoices, lease agreements, insurance documents and photographs.
6. All papers containing names, addresses, telephone numbers, email addresses and/or other contact information for storage facilities, clients, financial institutions, persons or other businesses with whom a business or financial relationship may exist;
7. All records of personally identifying information (genuine or fictitious);
8. Cellular telephones and portable digital assistants, along with their power cords, user manuals and software;
9. Telephone records (including both cell phone and land line records) including contracts, invoices, and documents reflecting assigned phone numbers; and
10. Indicia of occupancy, residency, rental and/or ownership of the PREMISES or vehicles located thereon, including, but not limited to utility and telephone bills, canceled envelopes, keys, deeds, purchase lease agreements, land contracts, titles, and vehicle registrations.
11. Any computers, digital media, and items of electronic storage media, located in the bedrooms, home office, and/or common areas of the PREMISES, may be seized as instrumentalities, fruits, and evidence of the crime and forensically examined for the items specified in this Attachment to include;

- A. Evidence of who used, owned, or controlled the computer at the time the records or information described in this warrant were created, edited or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chats,” instant messaging logs, photographs, and correspondence;
- B. Attachments to the computer, such as data storage devices or similar containers for electronic evidence;
- C. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- D. Passwords, encryption keys, and other devices that may be necessary to access the computer, to include phone passwords;
- E. Documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- F. Records of or information about Internet Protocol addresses used by the computer;
- G. Records of or information about the computer’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that a user entered into any Internet search engine, and records of user-typed web addresses; and
- H. Contextual information necessary to understand the evidence described in this Attachment.
 - (1) The terms “records” includes all of the foregoing items of evidence in whatever form and whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard discs or other media that can store data); any handmade form (such as written); and mechanical form (such as printed, typed, recorded on a magnetic tape or digital audio file); and any photographic or photomechanical form (such as microfilm, microfiche, prints, slides, negatives, digital image file, videotapes, motion pictures, digital video files, or photocopies);
 - (2) The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones,

tablets, personal digital assistants, server computers, and network hardware; and

- (3) The term “data storage medium” includes any physical object upon which computer data can be recorded. Examples include, but are not limited to, hard disks, random access memory, floppy disks, flash memory, compact disks, subscriber identity module (“SIM”) cards, back-up tapes, device memory buffers, and other magnetic, optical, and solid state electronic media.
- 12. All records or other physical items related to purchases made using any bank account or credit card in the name of the Fire Department, including consumer goods, and photographs or other mementos of vacations, concerts, or other events.
- 13. All records related to fundraising for the Fire Department, including pull-tab games, bingo, raffles, and other such games and events.
- 14. All records related to BAKER’s management of the Fire Department, including in his roles as Secretary, Treasurer, Assistant Fire Chief, and Fire Chief.